TOASTMASTERS INTERNATIONAL

Guide to GDPR Compliance for Clubs

Nominate someone to own GDPR compliance. (We recommend the Club Secretary.)

Create a visual of your process for members to reference. Document these items:

- Where the data is
- How it is accessed
- Who has access
- How it is used

Present the privacy notice provided by WHQ to new members, guests, and current members at least one time. A consent section has been included in the statement. The club is to hold the consent page in its records as long as they hold the data.

Security

Computer

- Computers should have the latest security software updates.
- All information should be password protected.
- Computers where data is stored should have limited access.
- If a group or outsiders must have access, an encryption system is encouraged.

Cloud Services

- If information is kept on the cloud (an offsite storage facility managed by a third party accessed via an internet connection) we recommend asking the providers if their security is GDPR compliant.
- Dropbox, Google Drive and OneDrive are examples that have security measures built in.
- If you choose to use Cloud services, be informed on their data privacy standards.

Hard Copy

- Hard copy files should be kept in a secure lockbox.
- Access to this box should be limited to one or two people at most (such as the club president and secretary).

Additional Steps

Outside Vendors

- Any time member data is sent to a third party, clubs should take steps to obtain compliance statements from those entities.
- Examples: Listserv, cloud services and website hosting.

Data Retention

- Data should be held as long as an individual keeps their membership, or until they request it is erased.
- If an individual requests data erasure: 1) Erase all records of them within 72 hours. 2) Notify World Headquarters of your steps to document them. 3) Advise the individual to contact WHQ on their own if they would like to be deleted from Toastmasters completely.
- Financial information should be thoroughly deleted immediately after use.

Subject Access Requests

- An individual may request a copy of their personal data held by the club at any time.
- Data should be provided upon request without any undue delay.
- Log each of these requests.

Data Breach

Any data breach should be reported to the Information Commissioner's Office within 72 hours of discovery. World Headquarters should also be notified immediately.